

REMARKS

Applicant has carefully studied the outstanding Official Action. The present amendment is intended to be fully responsive to all points of rejection and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the present application are hereby respectfully requested.

Applicant thanks the Examiner for the courtesy of a telephonic interview granted to Applicant's representative, David Zviel, registration number 41,392, on 7 June 2004. Inventor Jordan Yaakov Levy also participated in the telephonic interview.

In the interview, the advantages of the present invention, as claimed in claim 1, over the prior art were discussed; the advantages which were discussed are described, for example, in the description on page 5, lines 8 - 10, and page 7, lines 1 - 8. The allowability of claim 1 over the prior art of record was also discussed briefly, along the lines of the full discussion below. The Examiner stated that, upon filing of a response, he would review the case with his supervisor and respond promptly.

Claims 1, 4, 6, 8, 14 and 15 stand rejected under 35 USC 103(a) as being unpatentable over Applicant's Admitted Prior Art (AAPA) in view of US RE 37,178 to Kingdon and further in view of US Patent 5,245,657 to Sakurai and further in view of US Patent 6,377,691 to Swift et al.

Sakurai describes a verification method and apparatus.

Kingdon describes a method and apparatus for authentication of client-server communication, which is intended to prevent the forging of message packets.

Swift et al describes a challenge-response authentication protocol intended for use with datagram-based remote procedure calls.

Claim 1 recites, inter alia, "the verifier sending an initialization message to the prover, the initialization message comprising a disguised form Y produced by applying a public disguising function Fp to Q and X, Y being equal to Fp(Q,X); the prover computing a random number R by applying a private disguising function Fv to Y, R being equal to Fv(Y); the prover sending a commit

message to the verifier, the commit message comprising a disguised form of R produced by applying a function f to R, the disguised form of R being equal to $f(R)$ ".

Applicant respectfully points out to the Examiner that at least the following features, recited in claim 1, are not found in any of the prior art of record. Since Sakurai is the closest prior art of record for the indicated features, each feature is contrasted to Sakurai:

1) The prover bases its commit message on an initialization message received from the verifier. In Sakurai, by contrast, a value generated by the verifier is used as a challenge value, not as a commit value.

2) The verifier uses a public disguising function; the prover applies a private disguising function F_v to the value received from the verifier. In Sakurai, by contrast, the verifier applies a digital signature function which, by definition, is a private and not a public function; there is nothing in Sakurai parallel to the prover's private disguising function as recited in claim 1.

3) The prover, by sending the disguised form R to the verifier, links a disguised challenge to the initial input. In Sakurai, by contrast, the verifier, by digitally signing the initial input, provides proof that the verifier accepted the prover request recorded in the transcript.

Applicant therefore respectfully points out that claim 1 recites a number of features which are not found in, and are in fact very different from, the prior art of record.

Claim 1 further recites that "the verifier choosing a challenge Q and a padding string X". As is clearly stated in the specification, in the first full paragraph on page 7, the padding string is randomly chosen by the verifier. The Examiner takes the position that Kingdon discloses the indicated limitation; Kingdon, however, as the Examiner points out, only discloses using zeroes as padding.

Claim 1 is therefore deemed allowable.

Claims 4, 6, and 8 depend from claim 1 and recite additional patentable subject matter and are therefore deemed allowable.

Claim 14 is a system claim corresponding to method claim 1 and is deemed allowable with reference to the above discussion of the allowability of claim 1.

Claim 15 is an apparatus claim corresponding to method claim 1 and is deemed allowable with reference to the above discussion of the allowability of claim 1.

Claims 2, 3, 5, 7, and 9 stand rejected under 35 USC 103(a) as being unpatentable over AAPA in view of Kingdon and further in view of Sakurai and further in view of Swift et al and further in view of US Patent 5,987,134 to Shin et al.

Shin et al describes a device and method for authenticating a user's access rights to resources, including a challenge - response and proof mechanism.

Claims 2, 3, 5, 7, and 9 depend directly or indirectly from claim 1 and recite additional patentable subject matter and are therefore deemed allowable.

Claim 10 stands rejected under 35 USC 103(a) as being unpatentable over AAPA in view of Kingdon and further in view of Sakurai and further in view of Swift et al and further in view of US Patent 6,076,163 to Hoffstein et al.

Hoffstein et al describes a secure user identification method using constrained polynomials.

Claim 10 depends from claim 1 and recites additional patentable subject matter and is therefore deemed allowable.

Claim 11 stands rejected under 35 USC 103(a) as being unpatentable over AAPA in view of Kingdon and further in view of Sakurai and further in view of Swift et al and further in view of Shin et al and further in view of Hoffstein et al.

Claim 11 depends indirectly from claim 1 and recites additional patentable subject matter and is therefore deemed allowable.

New claims 16 - 18, dependent respectively from claims 1, 14, and 15, have been added.

Each of new claims 16 - 18 recites that "the padding string X comprises randomly chosen padding". New claims 16 - 18 are supported, inter alia, by the first full paragraph on page 7 of the specification.

Applicant has carefully studied the other prior art of record including:

US Patent 6,044,463 to Kanda et al, which describes a message delivery system utilizing a zero-knowledge interactive proof protocol;

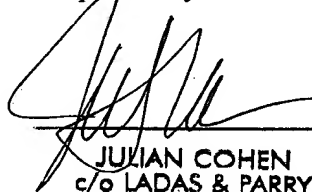
US Published Patent Application 2002/0002675 of Bush, which describes a secure encryption system using a one-time pad; and

US Patent 4,926,479 to Goldwasser et al, which describes a multiparty verification system using multiple provers.

Applicant finds that the present invention as claimed is neither described nor suggested in the prior art of record, taken either individually or in combination.

In view of the foregoing remarks, it is respectfully submitted that the present application is now in condition for allowance. Favorable reconsideration and allowance of the present application are respectfully requested.

Respectfully submitted,



JULIAN COHEN
c/o LADAS & PARRY
26 WEST 61st STREET
NEW YORK, N. Y. 10023
Reg. No. 20302 (212) 708-1887